summit
financial group

June 22, 2015

By US Mail

Re: DATA SECURITY INCIDENT YOUR PIN CODE:

Dear :

We are writing to you to inform you of a recent incident at Summit Financial Group ("Summit") that may have subjected your personal information, including your name, address, date of birth, and Social Security number to unauthorized access. This information may have been subjected to unauthorized access because you are listed as a dependent on your parent's/guardian's tax return and the information was contained on the tax return. Even though we believe that it is highly unlikely that this information has been used without authorization, we believe it is appropriate to share this information with you.

**What Happened**

After a Summit client files a tax return, we mail the client a CD that contains his or her tax return. Between January 1, 2015 and February 15, 2015, in connection with performing tax return services for our clients, we mailed CDs to sixty-seven clients. We intended that these CDs would contain only the individual recipient's tax return information. On April 15, 2015, a client contacted Summit to inform us that a single CD had other clients' data on it. We immediately retrieved that CD and confirmed that the individual had not retained any of the information on the CD. At that time, we had no reason to believe that any other CDs had information relating to other clients' tax returns stored on them. On May 15, 2015, one more client contacted us and informed us that the CD he/she received also contained other clients' tax return information. At that point, we learned that there had been an error by one of our employees when the CDs were compiled. As a result, we immediately began our investigation and started to personally visit each of the sixty-seven clients to retrieve all of the CDs issued between January 1, 2015 and February 15, 2015. All of the CDs have either been destroyed by our clients or personally collected by Summit where we are maintaining them in a locked container.

Through our investigation, we have learned that this incident, which affected a small number of Summit clients and their dependents, as applicable, was caused by human error. Your personal information may have been subject to unauthorized access because your parent's/guardian's tax return was on the CD and you are listed as a dependent on that tax return. During the process of compiling the CDs, one of our employees inadvertently copied data onto the CDs of eight other clients. The employee then failed to fully check the data prior to sending, which was inconsistent with Summit's policies and procedures. We also conducted a thorough analysis to review the data and determine what information was on the CDs in order to specifically identify the individuals we needed to provide notice to. We believe that approximately 662 individuals were affected.

**What We are Doing About It**

Although we have no evidence suggesting that your personal information has been misused, we take our obligation very seriously to keep your personal information confidential. We have taken aggressive steps to address this incident and protect your personal information, including the following:

- Reviewing our systems, processes and policies to determine what we can do to limit the exposure of personal information and further strengthen data security;
- Conducting a comprehensive physical security assessment;
- Implementing a new mandatory data security training program;
- Encrypting CDs sent from Summit that contain personal information; and
- Dismissing the employee responsible for the incident.

In order to help you monitor the possible misuse of your personal information, we are offering a *complimentary* two-year membership in CSID Protector™ to provide free credit monitoring. These services help detect possible misuse of your personal information and provide you with identity protection services focused on identification and resolution of identity theft. More information on this service, including how to activate this free service, is included in the attachment to this letter. Your **pin code** is shown at the top of this letter.

**What Can You Do**

Although we have no information at this time indicating that personal information, including your Social Security number, was inappropriately used by anyone, we are notifying you out of an abundance of caution so that you may take steps to protect yourself. We encourage you to remain vigilant and to contact us in the event you learn of any unauthorized use of your personal information. You should remain alert to unusual emails or other correspondence as well as any irregularities in your online personal accounts. We also recommend that you regularly review your credit reports and account statements for any unauthorized activity.

If you do find suspicious activity on your credit reports or become aware of identity theft, we recommend that you call your local law enforcement office and/or notify the Federal Trade Commission, file a police report of identity theft, and obtain a copy of the police report, as you may need to give copies of the police report to creditors to clear up your records.

If you would like to place fraud alerts and security freezes on your accounts you can contact Equifax, Experian or TransUnion at the numbers listed below:

| **Equifax** | **Experian** | **TransUnion LLC** |
|---|---|---|
| P.O. Box 105788 | P.O. Box 2104 | P.O. Box 2000 |
| Atlanta, GA 30348 | Allen, TX 75013 | Chester, PA 19022 |
| 1-800-349-9960 | 1-888-397-3742 | 1-888-909-8872 |
| www.equifax.com | www.experian.com | www.transunion.com |

For additional assistance on steps to avoid identity theft or to report an incident of identity theft, write to or call or visit the FTC's website listed below:

Federal Trade Commission
Bureau of Consumer Protection
Division of Privacy and Identity Protection
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580
1-877- IDTHEFT (1-877-438-4338)
http://www.ftc.gov/idtheft

Summit takes its responsibility to protect your personal information very seriously and has taken steps to help prevent something like this from happening again. We are thoroughly committed to the financial welfare and privacy of our clients and their families. If you have any further questions about the incident or the protections available to you, please contact me at 619-698-9760. We apologize for any inconvenience caused to you as a result of these events and want to reassure you that maintaining the confidentiality of your data remains a priority to us.

Very truly yours,

Della Taddeo

Della Taddeo
CEO, Summit Financial Group

Enclosure

**CSID Protector™ & CSID Child Monitoring/Cyber Agent Product**

In order to help you monitor the possible misuse of your personal information, we are offering a *complimentary* two-year membership in CSID Protector™ to provide free credit monitoring. These services help detect possible misuse of your personal information and provide you with identity protection services focused on identification and resolution of identity theft. Also included in this product is the CSID Child Monitoring/Cyber Agent Product. If applicable, this service monitors all known addresses and aliases associated with your child's SSN and alerts you if your child's personal information is being bought or sold online.

After you complete registration for CSID Protector™ coverage that Summit is providing for you at no charge, you will have increased visibility with respect to any possibly fraudulent activity regarding your identity so you can respond quickly if such activity is detected. We will also provide reimbursement under an identity theft insurance policy that will cover certain expenses that you incur up to $1,000,000 (subject to the terms and exclusions in such policy) should you become a victim of identity theft, and an Identity Restoration team to guide you through the recovery process. Summit encourages you to complete registration as quickly as possible before September 20, 2015 to take advantage of CSID Protector™ coverage.

The sign-up process is conducted online via CSID's secure website at:

http://www.csid.com/csidfamilyprotector2/

You will need your CSID **PIN CODE** shown at the top of the letter to complete registration. This PIN Code can only be used once and cannot be transferred to another individual. Once you have provided your PIN Code, you will be prompted to answer a few security questions to authenticate your identity, such as previous addresses, names of creditors and payment amounts. Once you register, you will have the option to enter a dependent's (i.e., your child's) information, if applicable. By entering your child's information and completing the related steps online, the CSID Child Monitoring/Cyber Agent product will be activated. Please note that should you not be able to complete the credit authentication piece of enrolling your child, you will be prompted to call CSID's Member Services Department where you will be required to provide documented proof of guardianship or power of attorney.

Should you have any questions regarding the coverage or the registration process, please contact CSID's Member Services Department at 1-877-274-5565 24/7 or email support@csid.com. Once you have enrolled and created your username and password, you will return to CSID's page to log in and access your personal information on future visits.

**CSID Protector™ includes the following services:**

- **Credit Monitoring:** Monitor your TransUnion credit file for credit inquires delinquencies, judgments and liens, bankruptcies, new loans and more.
- **CyberAgent® Monitoring:** CSID's Internet surveillance technology scours websites, chat rooms and bulletin boards 24/7 to identify trading or selling of your personal information online
- **Court Records Monitoring**: Know if and when your name, date of birth and Social Security number appear in court records for an offense that you did not commit
- **Non-Credit Loan Monitoring**: See if your personal information becomes linked to short-term, high-interest payday loans that do not require credit inquiries
- **Change of Address Monitoring**: Find out if someone has redirected your mail to get access to your bank statements, credit card statements and other important identity-related information
- **Sex Offender Monitoring**: Understand if and when any sex offenders reside or move into your zip code, and ensure that your identity isn't being used fraudulently in the sex offender registry
- **Social Security Number Trace Monitoring:** Know if your Social Security number becomes associated with another individual's name or address
- **Identity Theft Insurance**: You are reimbursed for certain specified expenses in the event that your identity is compromised, with coverage under a $1,000,000 identity theft insurance policy (subject to the terms and exclusions of such policy, and excluding New York residents)
- **Identity Restoration**: Work with a certified identity theft restoration specialist, who will work on your behalf to restore your ID and let you get on with your life
- **CSID Child Monitoring/Cyber Agent**: Monitors all known addresses and aliases associated with your child's SSN and alerts you if your child's personal information is being bought or sold online